RISK

MANAGEMENT

PLAN

Integrated Procurement System (IPS)

U.S. Election Commission

RISK MANAGEMENT PLAN

TABLE OF CONTENTS

Page #

1.0 RISK MANAGEMENT METHODOLOGY

Risk is managed by identifying, assessing, mitigating and tracking potential threats to project success.

1.1 Risk Identification

A risk is the likelihood that a particular threat to the system will actually occur and is identified as a potential for loss. Each phase of the project will include review of current and planned activities to identify potential risks. Individual responsibility for these reviews will be assigned based on expertise and availability.

1.2 Risk Assessment

The level of risk is rated as high, medium, or low, based on the following factors:

- ?? The magnitude of potential harm caused by the risk
- ?? The probability of harm resulting in denial of service, unauthorized disclosure, modification, or destruction of sensitive or critical data or resources
- ?? The probability of the threat occurring
- ?? The criticality of the system components that may be exposed to exploitation.

The ratings of “high”, “medium”, and “low” are qualifying terms that represent the degree, or level of risk to which a system may be exposed. An observation estimated to be of a high risk indicates that the system is highly vulnerable and if the risk event occurs, it will severely impact the system. It connotes a strong need for corrective measures and actions. An observation rated as having a medium risk is reasonably likely to occur and the degree of impact if the risk event occurs is moderate. An observation of low risk indicates that the identified weaknesses may occur, and that the risk event may cause minor harm to the system.

1.3 Risk Analysis and Mitigation

The purpose of assigning a risk level to each observation is to assist the USEC in managing risk. It allows the USEC management to prioritize the actions that will be necessary to mitigate the identified risks. A monthly report will be prepared showing the current assessment of each major risk identified below, other risks identified in this plan, and any emerging risks. Resolved risks will be deleted from the report. The report will be used to provide management attention to each risk in the program.

1.4 Risk Tracking

Each identified risk will be recorded in the tracking log and tracked as an individual item. A summary of all potential risks will be maintained in summary form and reviewed monthly by the project manager and project sponsor.

2.0 ROLES AND RESPONSIBILITIES

Each member of the IPS development and management team will perform risk analysis and risk response throughout the systems development lifecycles. Based on the scope the IPS project, these activities will focus on project management, systems development, software testing, and systems integration. The risk management activities to be performed by the team will also include but will not be limited to conducting/participating in regularly scheduled project status reviews, milestone reviews, systems development lifecycle reviews, and evaluating and reporting on project performance. These risk management activities will also involve identifying and implementing risk reduction measures. The following table outlines a risk management responsibility matrix that takes into consideration IPS systems development activities, the current team structure, and relevant organizational interfaces.

Table 1 Risk Management Responsibility Matrix

	IPS Project Activities								
Stakeholder	Initiate/Plan Project	Define Reqs.	Design System	Acquire SW	Acquire HW	Develop/ Doc./Unit Test System	Integrate and Test System	Install/Deploy /Train	Operate System
USEC									
Project Sponsor	P	P	S						P
Project Manager	P	P	P	P	P	P	P	P	P
OPC Users	P	P	S			S			S
Contractor									
Task Leader	P	P	P	P		P	P	P	P
Sr. Systems Analyst	S	P	P			P	P	P	
Sr. Programmer Analyst(s)	S	P	P			P	P	S	
DBA		S	P			S	S	P	S
Data Modeler	S	S	P	S	S	P	S	S	S
Technical Writer	S	S	S	S	S	P	S	S	S
Configuration Manager						P	P	P	P

P=Primary S=Secondary

3.0 RISK IDENTIFICATION

Early identification of project risks is paramount to the success of any project. Early identification provides sufficient time to analyze, plan, monitor, and control risks. If risks are identified and documented early, the process of assessing risk probability/impact and the steps required mitigating the risk could be relatively straightforward.

3.1 Identification Process

The IPS team's risk identification process will comprise the following four steps:

1. The project manager, team lead or designated team member identifies activities to be reviewed and personnel responsible
2. The project leader or designated team member for the activity to be reviewed will distribute review materials to participants.
    a. The review will be conducted in compliance with USEC standards and guidelines, and will focus on assessing alignment with project objectives and identifying functional and technical issues and concerns
3. Following each assessment, the reviewers will document findings on the proper template.
4. Identified risks will be reviewed with Project Sponsor.

3.2 Risk Identification by Phase

The following sections provide a list of activities that will be assessed during each phase of the development of IPS. Additional activities may warrant assessment and should be identified as appropriate.

3.2.1 Initiate/Plan Project

Activity	Risk Analysis
Needs Statement	Assess continued need for the Integrated Procurement System project
IPS project plan (includes project schedule and WBS)	Assess risks in project scope, tasks and resource assignments
Cost/Benefit Analysis	Review assumptions for system alternatives for lower risk approaches
Configuration Management Plan	Assess risk to change control process
Quality Assurance Plan	Assess risks to quality assurance and quality control guidelines for all project activities and deliverables
Feasibility study	Review assumptions and risks for functional, and/or performance objectives, and feasibility of the IPS implementation

Quality control measures	Assess the ability to obtain the metrics to be used to evaluate product and process quality

3.2.2 Define Requirements

Activity	Risk Analysis
System specifications	Assess the hardware and software risks for implementing IPS
System support and acquisition plan (initial)	Assess any additional hardware or software support requirements for the implementation and operation of IPS
Functional requirements document (FRD)	Assess the practicality of the user and business requirements that drive the development and implementation of IPS
QA requirements review, analysis and recommendations	Assess the QA review and process audit requirements
Data requirements document	Assess the data base structure and data integration requirements for IPS
System security and privacy plan	Assess the security and privacy requirements of relevant standards and laws
Internal Audit Plan	Assess the potential of IPS audits to identify risks in a timely fashion

3.2.3 Design System

Activity	Risk Analysis
System/Subsystem Specifications	Assess the technical issues with the detailed design of IPS
Data Requirements Document	Assess the analysis of data and associated system and functional requirements
Database design document	Assess the database's logical models and data integrity requirements
Database Specifications	Assess the detailed design for the system's databases
Program Specifications	Assess the functions, timing requirements, interfaces, input and output reports and the accuracy and validity requirements
System Support and Acquisition Plan (final)	Assess hardware and software support requirements
Validation, Verification, and Testing Plan (initial)	Assess IV&V process audit strategy and system testing strategy
Training Plan (initial)	Assess training methodology, tools, and schedule

	schedule

3.2.4 Acquire Software

Activity	Risk Analysis
Software review process assessment	Assess the software review and acquisition process

3.2.5 Acquire Hardware

Activity	Risk Analysis
Hardware service agreements	Assess service level agreements for life cycle impacts
System environment report	Assess the current operating systems, systems applications and associated infrastructure for potential interface issues

3.2.6 Develop, Test and Document System

Activity	Risk Analysis
Installation and Conversion Plan (initial)	Assess tasks to be performed to implement system as well as data conversion strategy
Test Plan	Assess unit and integration testing requirements and schedule
Operations Manual	Assess systems operations issues
Maintenance Manual	Assess system maintenance requirements
Problem/issues tracking and resolution report	Assess problems/issues identified during peer reviews

3.2.7 System Integration and Testing

Activity	Risk Analysis
Test Results and Evaluation Reports	Assess testing process, procedures and outcomes

3.2.8 Install, Deploy and Train

Activity	Risk Analysis
IPS Users' Manual	Assess IPS user functions and procedures
Acceptance testing report	Assess IPS acceptance testing procedures and results
Release procedures and deviations and waivers assessment	Assess IPS release policies and procedures

3.2.9 Operate System

Activity	Risk Analysis
SDM technical review report	Assess compliance with SDM process requirements
Pilot Test Results	Assess results of pilot testing activities
Disaster/recovery procedures	Assess system recovery and backup plans and procedures
System performance reports	Assess performance results from systems operations

4.0 ANALYSIS AND ASSESSMENT

The second risk management step is to analyze the identified risks. This activity generates information to characterize the risk, and leads to the development of the risk control strategy. The strategy will define the project intention to avoid, accept, mitigate, or transfer the risk. This analysis involves describing the risk, estimating its impact, and estimating the probability of occurrence. If necessary, a contingency plan is developed to support the avoidance, acceptance, mitigation, or transfer of the risk.

4.1 Scoring and Interpretation

It is important to document the probability of the risk occurring, the potential impact if it does occur (high, medium, or low), thereby arriving at the overall risk rating. It is also necessary to determine the owner of the risk—which area, group, or individual does the risk item potentially impact. The following table categorizes the probability of the risk event occurring.

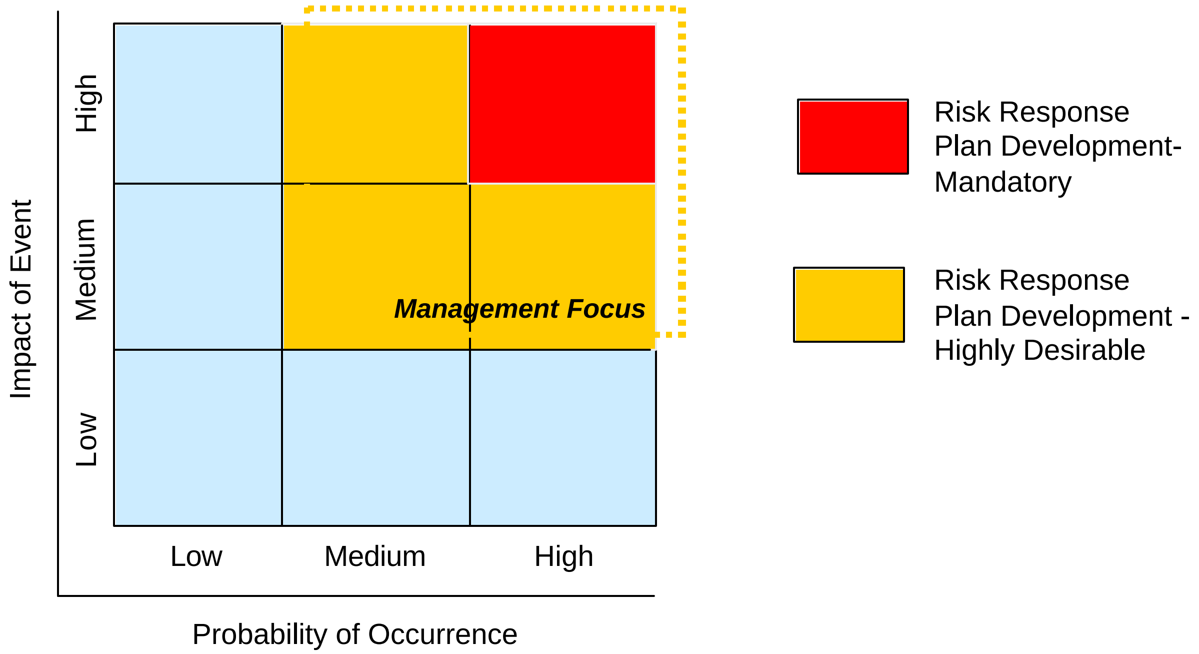
Probability	Relative Values
High	There is a 60% - 100% chance the risk will occur
Medium	There is a 30% - 60% chance the risk will occur
Low	There is a 0% - 30 % chance of risk will occur

Risk impact can be identified using the following classifications:

Category	Cost	Schedule	Performance
Critical (High)	Greater than 10% of Costs	Greater than 10 day delay	Breach threshold* value for greater than 10 days.
Marginal (Medium)	2-10% of costs	4-10 Day delay	Breach threshold value for 4-10 days
Negligible (Low)	Less than 2% of costs	1-3 Day delay	Breach threshold value for 1-3 days

* The clearly defined accepted measures of project performance.

The result of evaluation of impact and probability should then be assessed for overall impact using the following matrix:


Impact of Event
High
Medium
Low
Management Focus
Low
Medium
High
Probability of Occurrence
🟥 Risk Response Plan Development-Mandatory
🟨 Risk Response Plan Development - Highly Desirable

4.2 Risk Categories

Each of the potential risks identified for IPS are categorized by type of risk: strategic, technological, or project management. The overall assessment score for each of the potential risks described below is summarized in Section 7.

4.2.1 Strategic Risks

?? The new administration's business strategy introduces changes that extend the scope of the project's data capture requirements.

?? Users in the 25 remote locations resist making internal process changes needed to accommodate the new system.

4.2.2 Technological Risks

Using commercial-off-the-shelf components minimizes technological risk. However, the following potential risks have been identified.

?? New upgrade to network changes the technical requirements for the new system. Commercial-off-the-Shelf (COTS) obsolescence is expected to be a significant problem both for the network and the IPS. Continuous monitoring of equipment during the configuration management process will be necessary to identify purchases that can work with both old and new equipment.

?? System requirements analysis indicates non-standard data formats among required system interfaces. IPS is dependent on interfacing with other systems to distribute information. Additionally, the interface requirements to make this work have not been fully defined. Issues such as security, control of data, and protocols need to be addressed.

4.2.3 Project Management Risks

?? Project receives partial funding during budget review.

?? Unable to acquire the required specialized skils for the project in the time frame needed.

?? Project experiences schedule delays due to unforeseen difficulties in acquiring hardware. Since the design is made of existing commercial components, the primary equipment schedule risk is the availability of items on the bill of materials. With the large commercial market involved, experience indicates that some items will be delayed but that is measured in days or weeks, hardly ever in months or years.

4.3 Thresholds

If a risk item is assessed as being in the upper right cell (high probability x high impact), the project manager will prepare a risk contingency plan. If the risk is assessed as being in the adjoining three cells (high x medium) the project manager will evaluate the need for a risk contingency plan. Any other risk contingency plans can be prepared at the discretion of the project manager.

5.0 RISK CONTINGENCY PLANNING

5.1 Risk Control Process

Risk controlling is the process of initiating action to lessen the impact or probability of a risk event. Specific tasks for controlling a risk are defined based on a risk management strategy that considers the severity of the risk, project goals, and resource considerations. Possible risk management strategies include:

?? Accept – Take no action and accept the risk. (This is often an approach for low probability or low impact risks that are considered tolerable.)

?? Avoid - Take action to reduce the probability of risk occurrence

?? Transfer – Accept the risk but reduce the impact by sharing the costs with others

?? Mitigate – Take action to reduce the impact of the risk event

Potential risk management strategies are reviewed and approved by the team leaders and the project manager during the initial risk identification process. The status of the risk is reevaluated based on the risk mitigation action. The reevaluation consists of assessing the impact and probabilities of occurrence based on the mitigation strategy. Composing a mitigation strategy and tasks is the most difficult part of risk management. In most cases, identified risks will cross over into other areas of management. Managers must establish and mitigate potential interdependencies. The process requires the coordination and cooperation from the whole project team.

5.2 Risk Management Strategies

The following risk management strategies are planned for the risks identified above.

RISK DESCRIPTION	STRATEGY	PLANNED ACTIONS
Users in 25 remote locations will resist making internal process changes needed to accommodate the new system	Avoid	1. Establish and implement a robust Communications Plan for the initiative stressing the benefit to users. 2. Include field office representatives on the Integrated Project Team.
New Administration's business strategy introduces changes that extend the scope of data capture requirements.	Accept	None
Project delays due to unforeseen difficulties in acquiring hardware	Mitigate	1. Use an open system COTS package. 2. Identify multiple sources for hardware acquisition.
Unable to acquire the required specialized skills for the project in the time frame needed	Transfer	1. Require contractors to provide all specialized skills. 2. Include penalty and incentive clauses in the

		contracts.
Systems requirements analysis indicate non-standard data formats among required system interfaces	Avoid	1. Conduct an in-depth analysis of data structure of systems with which IPS will interface. 2. Work with managers of those systems to establish standard data formats which are enforced.
New upgrade to network changes the technical requirements for the new system	Avoid and Mitigate	1. Inform the Office of Network Services of the technical requirements of the new system to influence decisions which may impact the new system. 2. Immediately review and modify system specifications if it becomes apparent that network changes will impact the new system.

5.3 Risk Approval

The Risk Manager compiles all information associated with the identified risk and provides it to the Project Manager for final review and approval. The Project Manager assigns a priority ranking to each risk by adjudging the impact and the probability along with the importance and the criticality to the associated project. The Project Manager maintains a list of the top ten program risks in the Project Notebook and ensures that those risks are closely monitored to ensure the success of the project.

6.0 REPORTING FORMATS

Risk Events will be identified and reported in the following formats.

<table>
<tr><td colspan="9"><b>1. Risk Description:</b></td></tr>
<tr><td colspan="3"><b>Risk Probability</b></td><td colspan="3"><b>Impact</b></td><td colspan="3"><b>Overall Risk to Project</b></td></tr>
<tr><td>Low</td><td>Medium</td><td>High</td><td>Low</td><td>Medium</td><td>High</td><td>Low</td><td>Medium</td><td>High</td></tr>
<tr><td colspan="9"></td></tr>
<tr><td><b>Action:</b></td><td colspan="2">Mitigate</td><td colspan="2">Accept</td><td colspan="2">Avoid</td><td colspan="2">Transfer</td></tr>
<tr><td colspan="9"><b>Describe Impact on Project:</b></td></tr>
<tr><td colspan="9"><b>Risk Management Strategy:</b></td></tr>
</table>

Risk Event Summary Log

Risk #	Risk Event Description	Risk Probability			*Describe Impact on Project*	Impact Probability			Overall Risk to Project			
		Low	Med	High		Low	Med	High	Low	Med	High	
1.												
2.												
3.												
4.												
5.												
6.												
7.												
8.												
9.												
10.												
11.												

7.0 RISK TRACKING

Risk management does not end when a risk management strategy is approved. The risk manager and the responsible risk owner review each risk to ensure that the information is current. The review ensures that once a trigger event has occurred, the risk management strategy is reducing the negative impact to the project. If this is not the case, then the risk management strategy should be reengineered to provide a more effective strategy. While risks with high impacts and probabilities require substantial attention, risks with low impacts and probabilities also need monitoring. Monthly progress reports should be forwarded to the Program Manager detailing the status of each risk identified.

7.1 Tracking Assumptions/Issues

During the execution phase of the project, the assumptions, which did not turn into risks, must be monitored. The assumptions will either turn into a risk and must then be treated as such, or will be proven to be exact and are no longer an assumption. However, during execution, new issues might arise. These issues will also have to follow the process of assumption analysis.

7.2 Risk Controlling

The Project Manager has the overall responsibility for risk management and is responsible for final approval of all analyses. The Risk Manager is responsible for the maintenance of the risk management documentation including this Risk Management Plan.

The Team Managers are responsible for managing the risks within their respective areas of responsibility. They also provide the feedback on all risks outside their responsibility as identified by the program office. Finally, the Team Managers will act as the primary monitor for risks within their area of responsibility.

8.0 APPENDIX – COMPLETED RISK DESCRIPTIONS

Initiative Name: **Integrated Procurement System**

Risk #1:

Description: New administration's business strategy introduces changes that extends the scope of project's data capture requirements

Category:	Strategic ✍	Project Management	Technological
Probability:	High	Medium ✍	Low
Impact:	High ✍	Medium	Low
Action:	Accept ✍	Transfer	Mitigate

Risk Management Strategy:

Owner: Project Sponsor

Risk #2:

Description: Users in the 25 remote locations resist making internal process changes needed to accommodate the new system

Category:	Strategic ✍	Project Management	Technological
Probability:	High	Medium	Low ✍
Impact:	High	Medium ✍	Low
Action:	Accept	Transfer	Mitigate ✍

Risk Management Strategy:
Convene ongoing working group of users to serve as advisors throughout the system's development life cycle. Involve users during demonstration of the prototype. Conduct pilot program at various remote locations.

Owner: Project Manager

Risk #3:

Description: New upgrade to network changes the technical requirements for the new system

Category:	Strategic	Project Management	Technological ✍
Probability:	High	Medium ✍	Low
Impact:	High	Medium	Low
Action:	Accept	Transfer	Mitigate ✍

Risk Management Strategy:
Meet with network manager in Computer Services organization and discuss projected 5-year plan for network management and upgrade. Incorporate potential technical changes into current technical requirements for the new procurement system. Ask to be included in future network planning meetings.

Owner: Project Manager/Project Leader

Risk #4:

Description: Systems requirements analysis indicate non-standard data formats among required system interfaces

Category:	Strategic	Project Management	Technological ✍
Probability:	High ✍	Medium	Low
Impact:	High ✍	Medium	Low
Action:	Accept	Transfer	Mitigate ✍

Risk Management Strategy:
Use tool/technologies that support open architecture and provide data conversion capabilities

Owner: Project Leader/DBA/Data Modeler

Risk #5: **Description:** Integration testing reveals a major bug that will impact project schedule			
Category:	Strategic	Project Management	Technological ✍
Probability:	High	Medium ✍	Low
Impact:	High ✍	Medium	Low
Action:	Accept ✍	Transfer	Mitigate
Risk Management Strategy: **Owner:**			
Risk #6: **Description:** Project receives partial funding during the budget review			
Category:	Strategic	Project Management ✍	Technological
Probability:	High ✍	Medium	Low
Impact:	High ✍	Medium	Low
Action:	Avoid	Transfer	Mitigate ✍
Risk Management Strategy: Re-scope project tasks to accommodate project priorities that will be supported by the level of funding provided **Owner: Project Manager**			

Risk #7:

Description: Unable to acquire the required specialized skills for the project in the time frame needed

Category:	Strategic	Project Management ✍	Technological
Probability:	High	Medium	Low ✍
Impact:	High	Medium ✍	Low
Action:	Accept	Transfer ✍	Mitigate ✍

Risk Management Strategy:
Develop an inventory of the skills of internal staff and define individual training goals training goals that can develop the specialized skills needed to support the project. Maintain a list of vendors with the appropriate core competencies.

Owner: Project Manager/Project Leader/Project Coordinator

Risk #8:

Description: Project experiences schedule delays due to unforeseen difficulties in acquiring hardware

Category:	Strategic	Project Management ✍	Technological
Probability:	High	Medium	Low ✍
Impact:	High	Medium	Low
Action:	Accept	Transfer	Mitigate ✍

Risk Management Strategy:
Initiate hardware purchase requisition earlier than scheduled in the project plan.

Owner: Project Manager/Project Leader